Class 1: Introduction

Plan

1. Find your team, introduce yourselves and figure out a management structure and plan.
2. Bid for your role:
   T (lead Class 2: oracle padding attacks)
   L (blog Class 1/lead 3: breaking weak asymmetric crypto, Drown)
   S (lead Class 4: certificates)

Examining Certificates

1. When does the certificate for https://whitehouse.gov expire?
2. (won't be able to answer this until later today) Does the new adminstration's https://whitehouse.gov site use the same private key as Obama's? (What should the answer to this question be?)

First Few Milliseconds

Jeff Moser's *The First Few Milliseconds of an HTTPS Connection*

1. Install Wireshark.
2. Start Wireshark, and look at all the TLS sessions running on your laptop. How many different TLS sessions are there?
3. Pick one of the TLS sessions and try to figure out what application is using it. Who are the endpoints?
4. Assuming (for now!) the encryption is all perfect, what could someone intercepting the traffic learn?
5. What differences can you observe compared to what is described for the TLS 1.0 connections on that web page?

 Creative Commons Attribution-Noncommercial-Share Alike 3.0